

Cyber-Attacken proaktiv begegnen – So schützt die digitale Brandmeldeanlage von Sophos

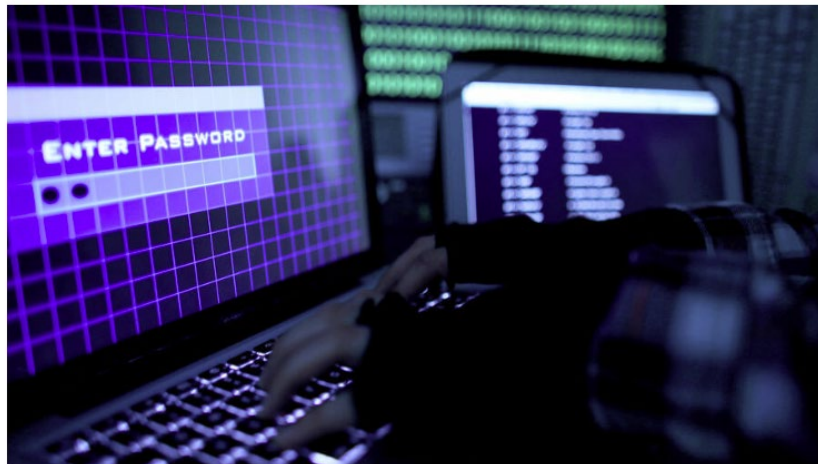
BITKOM-STUDIE

Russische Cyberattacken auf deutsche Unternehmen steigen sprunghaft an

Nahezu die komplette deutsche Wirtschaft ist laut einer Studie des Digitalverbands Bitkom von den Attacken betroffen. Die Angriffe kommen immer häufiger aus Russland und China.



Dietmar Neuerer

31.08.2022 • Update: 31.08.2022 - 13:05 Uhr • [Kommentieren](#) • [14 x geteilt](#)

Cybersicherheit

Vor einem erhöhten Risiko russischer Wirtschaftsspionage warnt auch der Bundesverfassungsschutz.
(Foto: dpa)

Berlin. Es gibt kaum noch Unternehmen in Deutschland, die von Cyberattacken verschont bleiben. Das zeigt eine an diesem Mittwoch veröffentlichte Studie im Auftrag des Digitalverbands Bitkom, für die mehr als 1000 Unternehmen quer durch alle Branchen repräsentativ befragt wurden. In den vergangenen zwölf Monaten waren demnach 84 Prozent der Unternehmen von Datenklau, Spionage oder Sabotage betroffen.

Die Angriffe aus Russland und China sind zuletzt sprunghaft angestiegen. 43 Prozent der betroffenen Unternehmen haben demnach mindestens eine Attacke aus China identifiziert (2021: 30 Prozent). 36 Prozent haben Urheber in Russland ausgemacht (2021: 23 Prozent).

Bitkom-Präsident Achim Berg sagte: „Spätestens mit dem russischen Angriffskrieg gegen die Ukraine und einer hybriden Kriegsführung auch im digitalen Raum ist die Bedrohung durch Cyberattacken für die Wirtschaft in den Fokus von Unternehmen und Politik gerückt.“ Die Bedrohungslage sei aber auch unabhängig davon hoch, genauso das Schadenpotenzial.

Insgesamt lag die Schadenssumme bei rund 203 Milliarden Euro pro Jahr – und damit etwas niedriger als im Rekordjahr 2021 mit 223 Milliarden Euro. In den Jahren 2018/2019 waren es erst 103 Milliarden Euro.

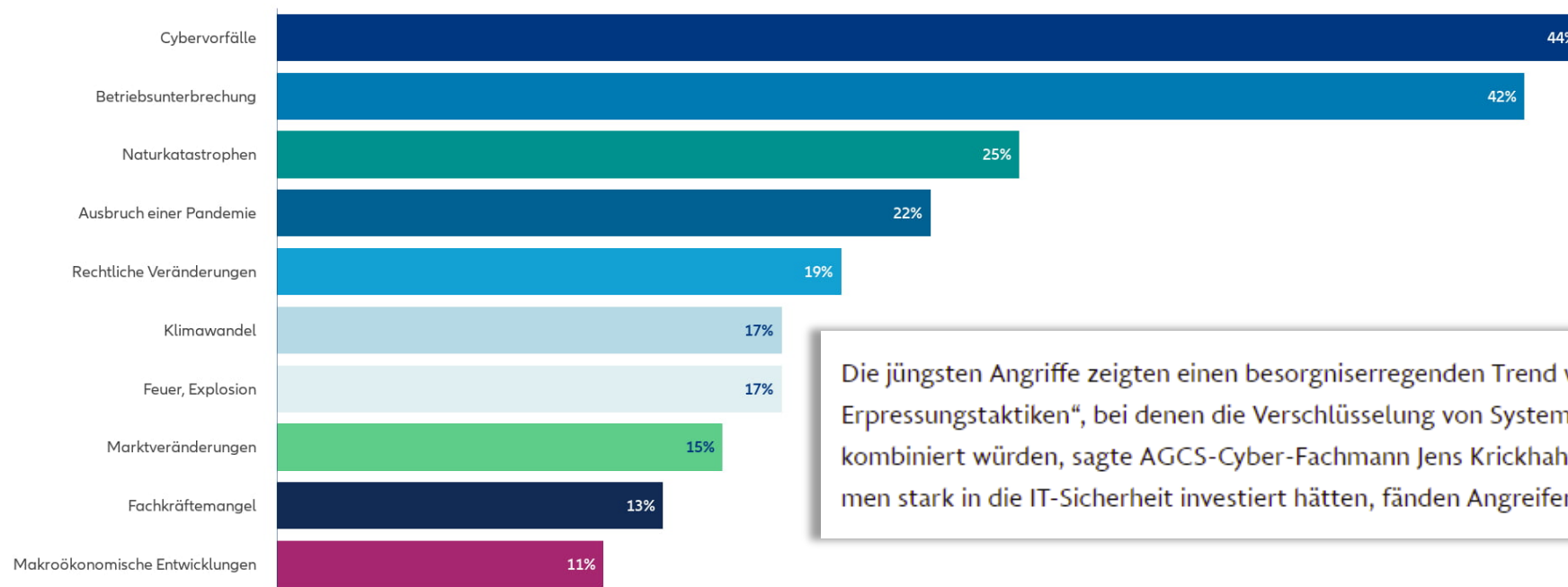
Vor allem Betreiber kritischer Infrastrukturen erleben immer mehr Angriffe: Hier sagen 49 Prozent, die Attacken haben stark zugenommen, und 38 Prozent, sie haben eher zugenommen. Die Sorgen vor den Folgen einer Cyberattacke wachsen laut der Bitkom-Studie: 45 Prozent der Unternehmen meinen demnach, dass Cyberattacken ihre geschäftliche Existenz bedrohen können – vor einem Jahr lag der Anteil bei gerade einmal neun Prozent.



Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Die jüngsten Angriffe zeigten einen besorgniserregenden Trend wie „doppelte Erpressungstaktiken“, bei denen die Verschlüsselung von Systemen mit Datendiebstahl kombiniert würden, sagte AGCS-Cyber-Fachmann Jens Krickhahn. Und obwohl viele Unternehmen stark in die IT-Sicherheit investiert hätten, fänden Angreifer immer wieder neue Lücken.

Bedrohungen nehmen zu in Menge, Komplexität, Schaden



57%

mehr **Angriffe** in den letzten 12 Monaten



66%

der SMB im letzten Jahr von **Ransomware** betroffen



11>15 Tage

Verweildauer im Netzwerk



4.3 Tage

zwischen **Datendiebstahl** und **Verschlüsselung**



90%

der Opfer hatten **Einschränkungen** des **Betriebes**



\$1.4M

Schaden pro Vorfall, vor allem durch Betriebsausfall

Cyber-Kriminelle heute = professionelle, brutale Verbrecher

WELT

POLITIK

DEUTSCHLAND

Mittwoch, 9. Juni 2021

Newsletter Podcasts Club ePaper Archiv Veranstaltungen

Handelsblatt

Branchen-News IT

NEWSLETTER ABONNIEREN

MEINE NEWS HOME POLITIK UNTERNEHMEN TECHNOLOGIE FINANZEN MOBILITÄT

CYBERKRIMINALITÄT


Todesfall nach Hackerangriff Düsseldorf

Eine Patientin stirbt, nachdem ihr Rettung einer Cyberattacke umgeleitet werden konnte. Das illustriert die wachsenden IT-Risiken im Gesundheitswesen.

Christof Kerkmann

Lars-Marten

18.09.2020 - 13:05 Uhr • Kommentieren • 12 x geteilt



Quelle: pa/Geisler-Fotopost/Snapshot/Tobias Seeliger/Geisler-Fotopress

heise online

heise+

IT Wissen Mobiles Security Developer Entertainment Netz


TOPTHEMEN: UKRAINE-KRIEG GOOGLE I/O WINDOWS 11 KRYPTOWÄHRUNGEN

heise online > News > 05/2022 > Nach Cyberangriff auf Fraunhofer-Institut in Halle Daten im Darknet angeboten

Nach Cyberangriff auf Fraunhofer-Institut in Halle Daten im Darknet angeboten

Hunderte Gigabyte an Daten sollen beim Fraunhofer-Institut für Mikrostrukturtechnik (IMT) im Darknet angeboten worden sein. Dem Institut wurde eine Lösegeldforderung gestellt.

Lesezeit: 2 Min. In Pocket speichern



(Bild: Oleksiy Mark/Shutterstock.com)


04.05.2022 18:04 Uhr
Von dpa

DIE RHEINPFALZ

SUCHE ANMELDE

MAINZ

Hackerangriff trifft auch Mainzer Stadtwerke



Hacker-Angriff auf IT-Dienstleister der Stadtwerke Mainz: Die Stromversorgung aber ist nicht betroffen.

symbolFoto: view - die agentur

WhatsApp Facebook Pinterest Email Print Link

dpa lrs

13. Juni 2022 - 14:18 Uhr

SOPHOS

Wie können Sie Cyberrisiken rechtzeitig vorbeugen?

Wer sagt, dass ich das wirklich brauche?

- Cyberrisikenversicherer
- DSGVO
- Regulierungsbehörden
- IT-Sicherheitsgesetz 2.0
- Während eines Vorfalls:
Jeder wünscht, es wäre schon da gewesen

Bundesverband IT-Sicherheit e.V.



IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

technischer und organisatorischer Maßnahmen

2021

3.2.22 Endpoint Detection & Response Plattform

Der Schutz der Endgeräte (z.B. PCs, Laptops, Smartphone oder Tablets) erfordert inzwischen weit mehr als nur ein Antivirus-Programm. Moderne Lösungen (Endpoint-Detection & Response Plattformen, EDR) vereinen neueste Schutztechnologien um alle Arten von Cyber-Angriffen auf Client und Server Systemen betriebssystemübergreifend zu stoppen und die Urheber zu identifizieren. Im Gegensatz zu konventionellen Lösungen ist kein spezifisches Vorwissen, wie z. B. Signaturen oder ein erstes Opfer nötig.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Malware
- Exploitation
- Maliziöse Scripte
- Hacker-Aktivitäten
- Missbrauch von Administrativen Werkzeugen und Tools in schädlicher Absicht

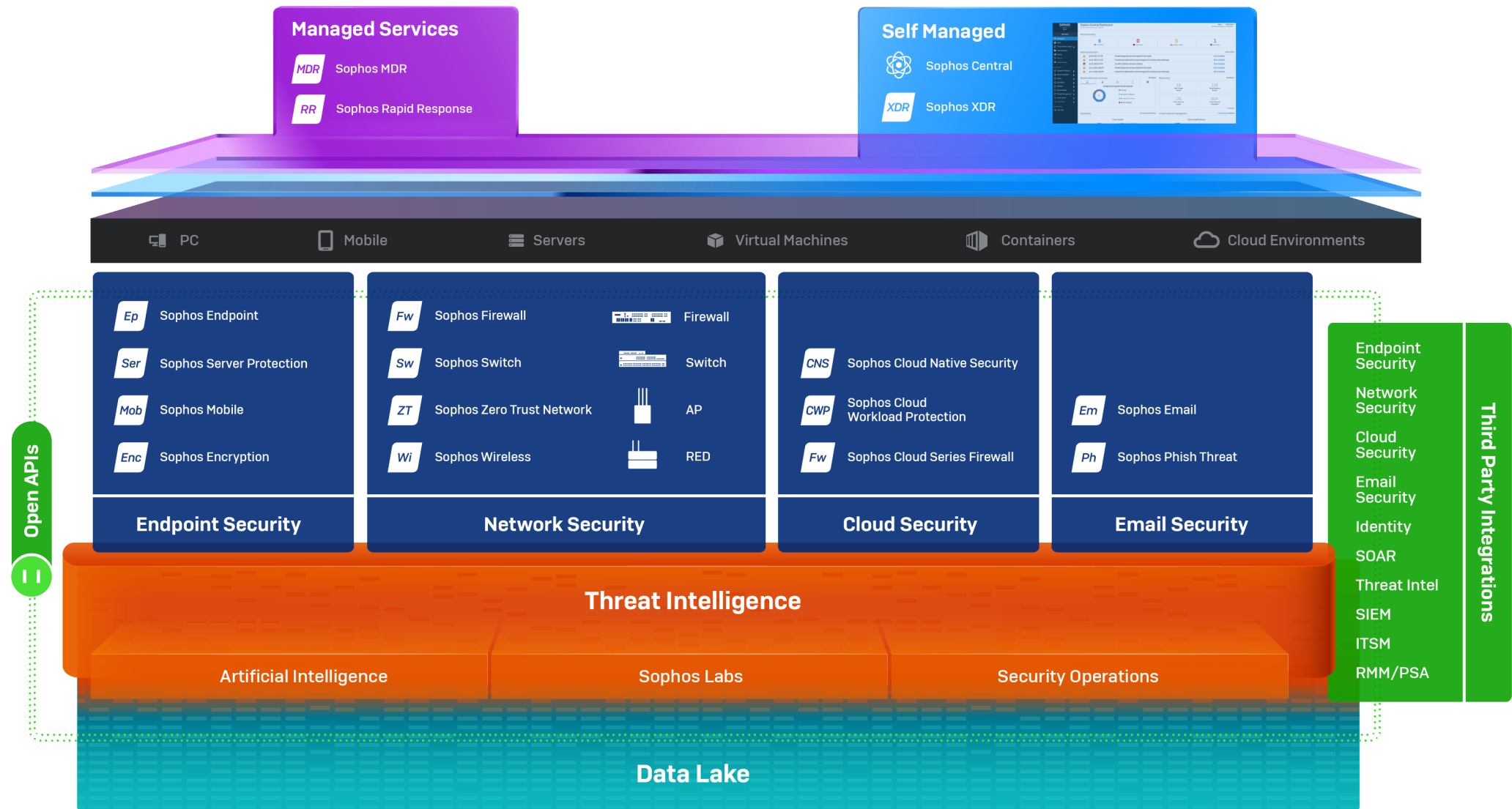
Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

EDR-Plattformen kombinieren wirksame Detektions- und Präventionstechniken, um die Kompromittierung von Clients und Servern, auch über Computer und Betriebssystemgrenzen hinweg, zu verhindern und sogar aktive Angreifer in Computernetzen zu enttarnen.

Komplexität ist der Feind von Sicherheit

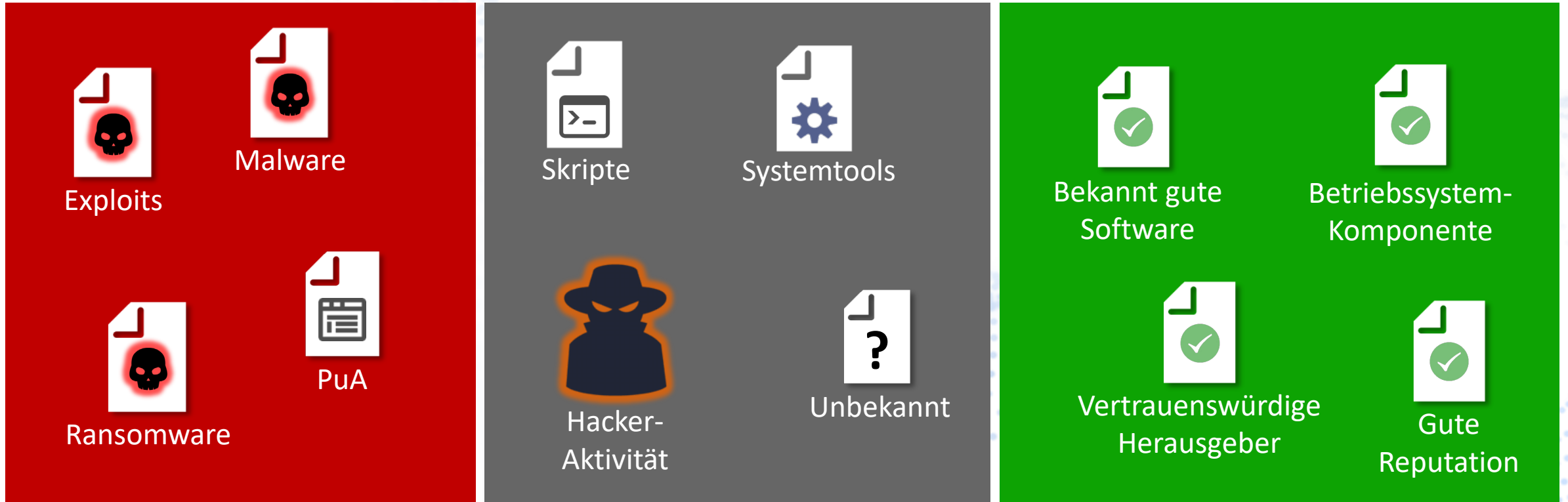


Adaptive Cybersecurity Ecosystem



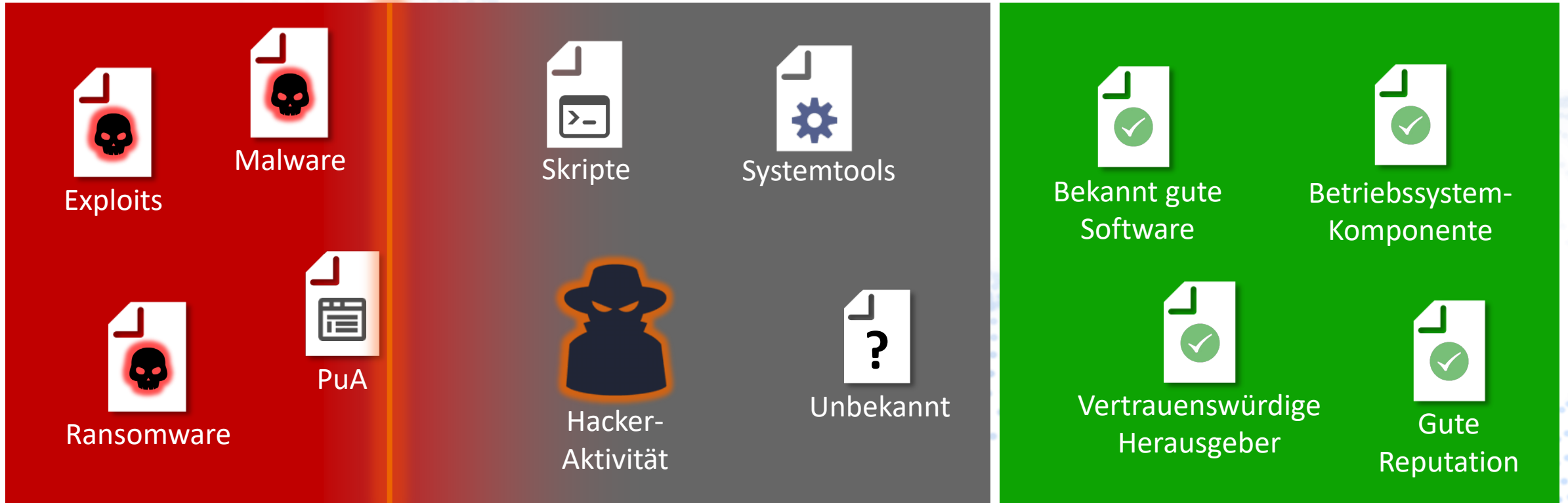
Was brauche ich heute?

Anti-Virus macht schon alles?



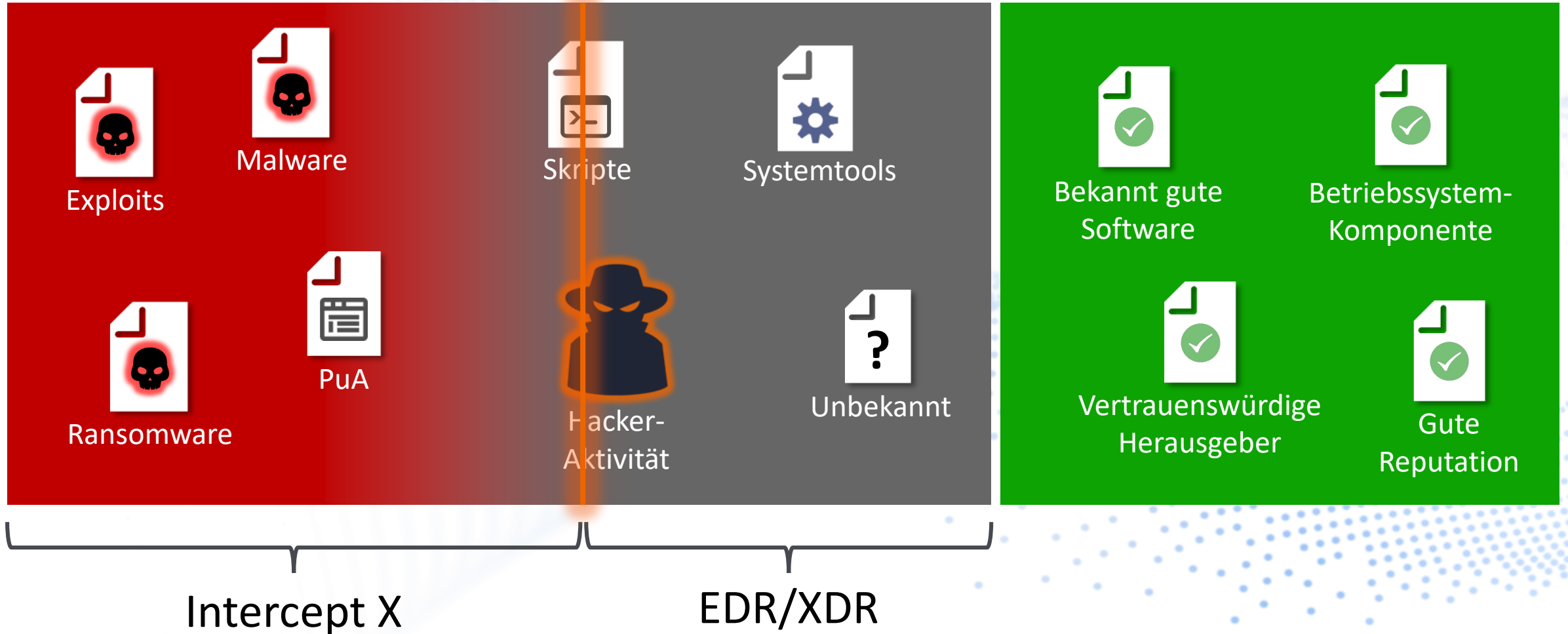
Sophos Realität

Wo setzt man die Grenze? -> Erkennung vs. False Positives!



Sophos Realität

Wo setzt man die Grenze? -> Erkennung vs. False Positives!



Bester proaktiver Schutz mit Intercept X



Einfallswege



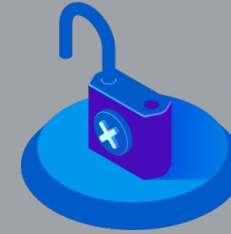
Exploit



Installation



Kommunikation



Aktionen



Pre-Breach

- Web Control
- Web Protection
- Intrusion Prevention System
- Network IPS
- Device Control
- Download Reputation
- Local Privilege Mitigation
- Application Lockdown
- Side Loading
- CTF Protocol
- Code Mitigations
- Memory Mitigations
- APC Mitigations

Post Breach

- Pre-execution Behavior
- Machine Learning
- Live Protection
- Anti-Malware
- Clean and Block
- AMSI
- Server Lockdown
- Process Protections
- PUA
- Application Control
- Credential Theft Protection
- Dynamic Shellcode
- Safe Browsing
- Malicious Traffic Detection
- Runtime Behavior Analysis
- Data Loss Prevention
- MFA Cookie
- Server File Integrity Monitoring
- Anti-Ransomware
- Automatic + Manual client isolation

Patchen - zeitnah!

Verschlüsselung

Awareness-Training

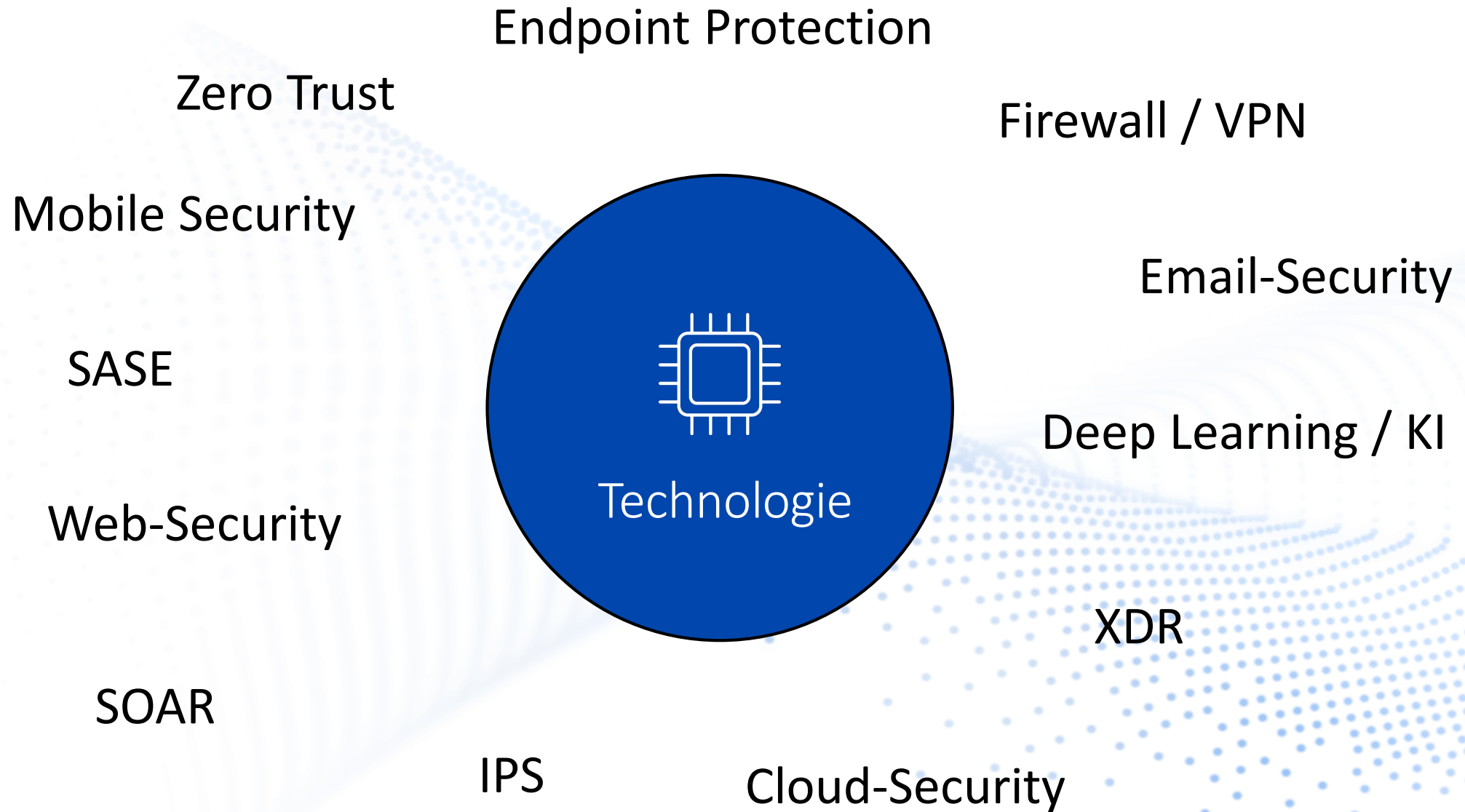
Multifaktor-
Authentifizierung



Netzwerksegmentierung

Backup

Schutz aller Geräte

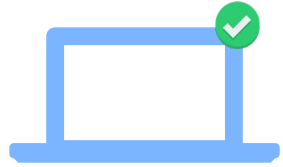


Was ist Sophos XDR ?

- Beste proaktive Schutztechnologien
- Erfassung, Analyse und Korrelation aller Technologien: Endpoint, Firewall, Cloud, Email, Netzwerk, Identität..
- Aussagefähigkeit
 - Cyberangriff?
 - Datenabfluss / Compliance-Verstoß?
 - Zustand der IT?
- Bei einem Vorfall: Fähigkeit zur Reaktion



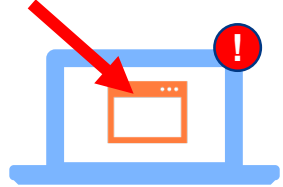
Sieht Ihr Netzwerk so aus?



✓ = verwaltet, EPP, gepatcht, aktuelles OS

..oder so?

“Tolles Tool” vom User selbst installiert



WLAN-Webcam, noch nie upgedatet



Privates älteres Android ohne Updates, ohne AV



Mitarbeiter, der auf jeden Link und Anhang klickt



Win7-Notebook “im Schrank”



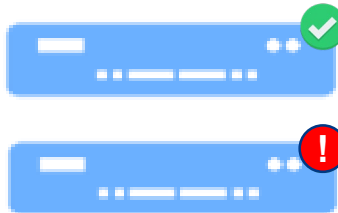
“später neu starten” geklickt



Privates Notebook



Reboot erst im nächsten Wartungsfenster



Server2003/2008 mit alter Software



Drucker/Scanner/Kopierer mit Windows Embedded ohne AV und Updates



Entwickler-Workstation mit vielen Scan-Ausnahmen



Maschinensteuerung mit NT 4.0/Win2000



! = unsicher

✓ = verwaltet, EPP, gepatcht, aktuelles OS



..oder so?

“Tolles Tool” vom
User selbst installiert

WLAN-Webcam,
noch nie upgedatet

Privates älteres Android
ohne Updates, ohne AV

Mitarbeiter, der auf
jeden Link und Anhang klickt

Win7-Notebook
“im Schrank”

..dann brauchen Sie

XDR

Privates Notebook

Server2003/2008
mit alter Software

Reboot erst im nächsten
Wartungsfenster

Drucker/Scanner/Kopierer
mit Windows Embedded
ohne AV und Updates

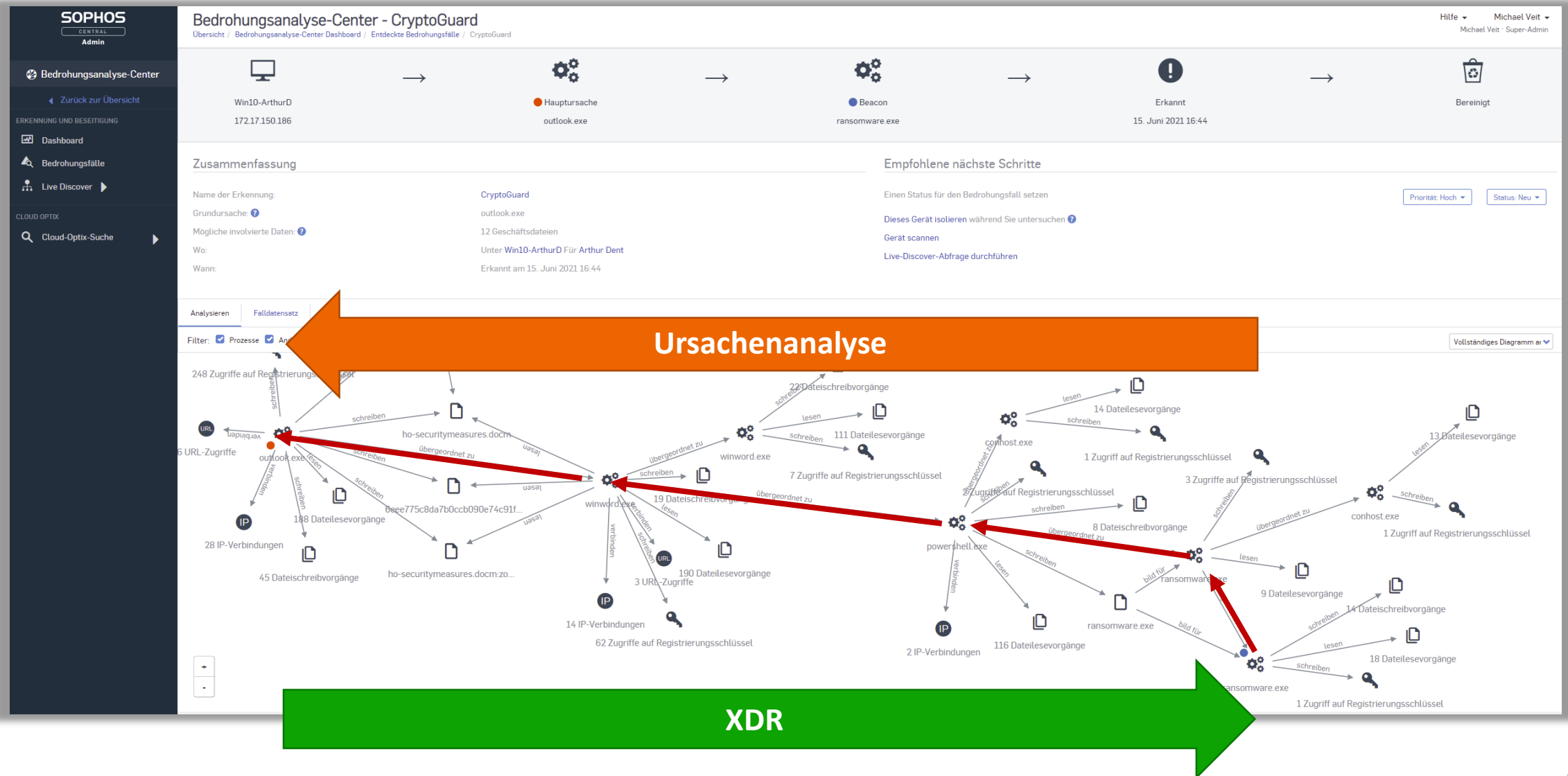
Entwickler-Workstation
mit vielen Scan-Ausnahmen

Maschinensteuerung
mit NT 4.0/Win2000

! = unsicher

✓ = verwaltet, EPP, gepatcht, aktuelles OS

Ursachenanalyse vs. XDR



XDR Erkennungen: KI sortiert verdächtige Ereignisse vor

Erkennungen

Überblick / Bedrohungsanalyse-Center Dashboard / Erkennungen

Hilfe ▼ Michael Veit ▼

Michael Veit · Super-Admin

Bedrohungsanalyse-Center

← Zurück zur Übersicht

ERKENNUNG UND BESEITIGUNG

Dashboard

Bedrohungsgraphen

Live Discover

Erkennungen

Analysen

CLOUD OPTIX

Cloud-Optix

Filter anzeigen

9 angewendet

Letzte Stunde

Letzte 24 Stunden

Letzte 7 Tage

Letzte 30 Tage

Maßnahmen ▼

Risiko	Anzahl	Kategorie	MITRE ATT&CK	Geräteliste	Erstmalig aufgetreten	Letztmalig aufgetreten	Beschreibung	Klassifizierungsregel
2	2	Bedrohung	Discovery System Information Discovery	Win10-ArthurD und mehr	28. Dez. 2021 21:30:00	28. Dez. 2021 21:32:56	Gpresult is used to enumerate domain policies.	EQL-EXEC-gpresult.exe
8	2	Bedrohung	Credential Access LSASS Memory	Win10-ArthurD und mehr	28. Dez. 2021 21:20:54	28. Dez. 2021 21:24:45	Adversaries can utilize living off the land techniques (Rundll32 comsvcs.dll MiniDump technique) or common 3rd party tools (Sysinternals ProcDump) to dump the LSASS...	EQL-WIN-CRD-PRC-LSASS-DUMP-1

Betriebssystem: Microsoft Windows 10 Pro

Angemeldeter Benutzer: michael

Übergeordneter Prozess: splunkd.exe

Übergeordneter Pfad: C:\Users\Public\splunkd.exe

Übergeordnete SonhosPID: 2272:132851943051301965

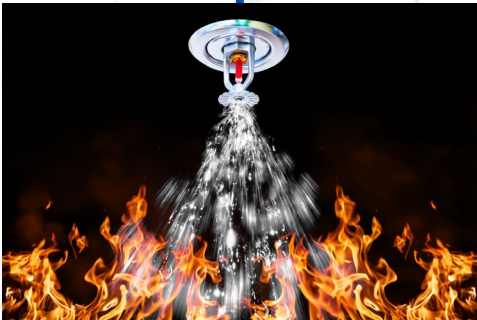
Aktionen

Einen Bedrohungsgraph erzeugen



Wie kann die digitale Brandmeldeanlage von Sophos helfen?

Managed Detection and Response



Was ist Sophos MDR?



24/7 Security Operations

- Threat Hunting
- Incident Response
- Proaktive Verbesserung der Sicherheit

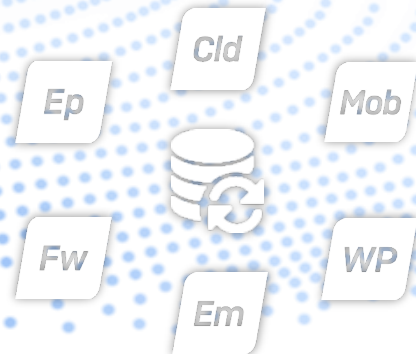
Flexible Deployment Optionen

Sie haben die Wahl – von „Do-it-Yourself“ bis „Full-Service“



Sophos Managed Detection and Response (MDR)

- Beinhaltet Intercept X with XDR
 - d.h. modernste proaktive Schutztechnologie
- plus Service d.h. Bedienung durch Sophos Experten für
 - 24/7 Angriffserkennung
 - 24/7 Stoppen und Beseitigung von Bedrohungen
 - 24/7 Threat Hunting und Incident/Response
- Proaktive Verbesserung der Sicherheit
- nutzt Ereignisse von Endpoints, Servern, Firewall, Cloud, ...
- All-inclusive: alle Fälle, Überwachung, Reaktion, Reporting etc.



Zusammenarbeit mit dem MDR Team



Benachrichtigung



Zusammenarbeit



Autorisierung

Sophos: „Auf diesen Weg
wir einen Angriff zu verhindern.
Aktivitäten feststellen.“

Kunde: „Danke, wir ü...

te stoppt jeden
Angriff!“
acht.“

Autorisierte Kontakte

Bedrohungsreaktion

Bedrohungsreaktionsmodus

Legen Sie fest, wie wir auf aktive Bedrohungen reagieren sollen.

- ☒ Benachrichtigen – Meine Kontakte sollen informiert werden, damit sie Maßnahmen ergreifen können
- ☐ Zusammenarbeiten – Zusammenarbeit mit meinen Kontakten
 - ☐ Ich ermächtige das MTR-Team, Maßnahmen zu ergreifen, falls meine Kontakte nicht erreichbar sind und eine aktive Bedrohung besteht. (Für Details siehe die [Service-Beschreibung](#))
- ☐ Autorisieren – Aktive Bedrohung beheben und meine Kontakte informieren (Hiermit wird das MTR-Team autorisiert, Maßnahmen zu ergreifen.)

Bedrohungsanalyse-Center

[Zurück zur Übersicht](#)

ERKENNUNG UND BESEITIGUNG

- Dashboard
- Bedrohungsgraphen
- Live Discover
- Erkennungen
- Analysen
- Einstellungen

Filter anzeigen

5 angewendet

Letzte Stunde

Letzte 24 Stunden

Letzte 7 Tage

Letzte 30 Tage

Aktionen ▾

ⓘ Diese Erkennungen dienen Ihnen als MTR-Kunde nur zur Informationen für alle Geräte mit MTR-Lizenz. Unserer MTR-Team wird Sie kontaktieren, falls Sie Maßnahmen ergreifen müssen.

	Risiko ▴ ▾	Anzahl ▴ ▾	Kategorie ▴ ▾	MITRE ATT&CK	Geräteliste	Erstmals aufgetreten ▴ ▾	Letztmalig aufgetreten ▴ ▾	Beschreibung	Klassifizierungsregel ▴ ▾	Analysen	
<input type="checkbox"/>	10	2	Classifier	Impact Data Encrypted for Impact	Win10-1	7. März 2022 01:31:59	7. März 2022 15:31:34	The adversary is trying to manipulate, interrupt, or destroy your systems and...	WIN-MITRE-Behavioral-TA0040-T1486	2022-03-07-0... und mehr	▾
<input type="checkbox"/>	8	2	Classifier	Defense Evasion Process Hollowing	Win10-1	7. März 2022 01:31:59	7. März 2022 15:26:25	The adversary is trying to avoid being detected. Defense Evasion consists...	WIN-MITRE-Behavioral-TA0005-T105...	2022-03-07-0... und mehr	▾
<input type="checkbox"/>	8	3	Bedrohung	Defense Evasion Mshta	Win10-1 und mehr	7. März 2022 01:11:05	7. März 2022 15:24:11	This detection looks for MSHTA connecting to a URL. This is a living off the...	EQL-WIN-EVA-PRC-MSHTA-HTTP	2022-03-07-0... und mehr	▾
<input type="checkbox"/>	7	1	Bedrohung	Execution Windows Management Instrumentation ...	Win10-4	-	7. März 2022 01:40:38	Ransomware has leveraged Windows Management...	EQL-WIN-IMP-PRC-SHADOWCOPY-SE...	2022-03-07-0...	▾
<input type="checkbox"/>	7	1	Bedrohung	Impact Inhibit System Recovery	Win10-4	-	7. März 2022 01:40:38	Adversaries may delete or remove built-in operating system data and turn off...	EQL-WIN-IMP-PRC-VSSADMIN-DELET...	2022-03-07-0...	▾
<input type="checkbox"/>	8	2	Bedrohung	Discovery Domain Trust Discovery	Win10-4	7. März 2022 01:40:20	7. März 2022 01:40:20	The legitimate tool ADFind has been observed being used by ransomware cre...	EQL-WIN-DIS-PRC-ADFIND-1	2022-03-07-0...	▾
<input type="checkbox"/>	6	1	Bedrohung	Defense Evasion Windows File and Directory Permissions M...	Win10-4	-	7. März 2022 01:40:20	Identifies the use of 'icacls.exe' to grant full access to everyone on a...	EQL-WIN-EVA-PRC-ICACLS-GRANT-E...	2022-03-07-0...	▾
<input type="checkbox"/>	8	1	Bedrohung	Defense Evasion Regsvr32	Win10-4	-	7. März 2022 01:14:06	Uses regsvr32 to load unauthorized script objects.	EQL-WIN-EVA-PRC-REGSVR32-SCRO...	2022-03-07-0...	▾
<input type="checkbox"/>	6	1	Bedrohung	Command and Control Ingress Tool Transfer ...	Win10-4	-	7. März 2022 01:10:57	HTML Help is a built in Windows executable that can be used to download...	EQL-WIN-EVA-PRC-HTML-HELP-1	2022-03-07-0...	▾
<input type="checkbox"/>	6	1	Bedrohung	Defense Evasion InstallUtil	Win10-4	-	7. März 2022 01:10:57	Code can be executed through InstallUtil which can be used to bypass...	EQL-WIN-EVA-PRC-INSTALLUTIL-PRO...	2022-03-07-0...	▾

Managed Threat Response

Zurück zur Übersicht

ANALYSIEREN

Dashboard

Fälle

Berichtsverlauf

Benachrichtigungen

KONFIGURIEREN

Einstellungen

Aktualisieren Letzte 7 Tage

Gesamtzahl der Fälle 3 ↑ Von 0 in Vorperiode	Aktive Fälle 2 ↑ Von 0 in Vorperiode	Behobene Fälle 1 ↑ Von 0 in Vorperiode	Aktion erforderlich 2 ↑ Von 0 in Vorperiode
--	--	--	---

Fälle durchsuchen					
Kennung	Status	Fallerstellung	Schweregrad	Beschreibung	Zusammenfassung
106087	Aktion erforderlich	Feb. 5, 2022 at 12:10 PM	Wert 2	Threat Hunt - Proxyshell	<p>Sophos MTR team conducted a Proxyshell threat hunt on the estate. We have observed the creation of web shells on EC2AMAZ . We noticed the Exchange server host is not patched against the Proxyshell vulnerability and is vulnerable to exploitation. SAV has removed the malicious web shells but due to persistence still remaining on the host (in the form of config file entries, exchange certificate and mailbox export requests), the shells are keeping on replicating. Escalated to customer to remove persistence and patch the server.</p>
106066	Aktion erforderlich	Feb. 5, 2022 at 9:30 AM	Wert 3	Threat Hunt - Log4j VMWare Horizon	<p>The MTR team conducted an investigation across the estate for indications of vulnerable Log4j instances. After investigation, the MTR team did not identify malicious activity associated with the critical vulnerability in Apache Log4j. However, we identified instances of log4j which require patching. Escalated to customer with recommendations</p>
105049	Behoben	Feb. 1, 2022 at 11:27 AM	Wert 3	Threat Hunt - Malicious persistence	<p>The MTR Team has performed a leadless hunt across the estate and observed persistence of IsErik adware on the host Win10-3-LR. During our review, we observed a malicious domain and directory related to IsErik and persistence through a scheduled task. MTR has removed the scheduled task and persistent folder since the response mode was Authorize.</p>
« < 1 > » 10					

Reaktionsmaßnahmen



Maßnahme	Beschreibung
Konfigurationen ändern	Anpassen von Konfigurationen zur Verwaltung einer aktiven Bedrohung. Dies kann die Anpassung von Bedrohungsrichtlinien, die Aktivierung von EDR/MTR auf ungeschützten Geräten, die Anpassung von Ausschlüssen usw. umfassen.
Hosts isolieren	Nutzung der Sophos Central Funktion zur Isolierung von Hosts, um die Gefährdung eines kompromittierten Assets zu begrenzen
Dateien blockieren	Blockieren von Dateien durch SHA256 innerhalb einer Umgebung, um die Ausführung bösartiger Inhalte zu verhindern
Scan ausführen	System-Scan einleiten
Webseiten/IPs/CIDR sperren	Blockieren einer bestimmten Website oder IP-Adresse durch Web Control
Anwendung blockieren	Blockieren einer bestimmten Anwendung durch Anwendungskontrolle
Live-Terminal verwenden	Wenn andere Maßnahmen nicht greifen, können wir über das Live-Terminal direkt auf den Host zugreifen.

**Genehmigung durch den Teamleiter erforderlich.*

Managed Threat Response

[Zurück zur Übersicht](#)

ANALYSIEREN

[Dashboard](#)[Fälle](#)[Berichtsverlauf](#)[Benachrichtigungen](#)

KONFIGURIEREN

[Einstellungen](#)

Team,

Case ID: 2-106066**Date:** 2022-02-05 09:30:16 UTC**// Analysis:**

We have conducted an investigation across your environment for indications of vulnerable Log4j instances. After investigation, the MTR team did not identify malicious activity associated with the critical vulnerability in Apache Log4j. However, we identified the following instances of log4j which require your attention as some of them are End of Life and some are vulnerable to CVE-2021-44228:

Format Below: Hostname -Path -Log4j Version

- Win10-1 - C:\Xilinx\xic\tps\win64\jre\bin\java.exe - log4j-1.2.15.jar
- Win10-2 - C:\Users\armando.taveras\Downloads\arduino-1.8.16-windows\arduino-1.8.16\java\bin\javaw.exe - log4j-api-2.12.0.jar
- Win10-4 - D:\USERDATA\miguel.garabito\AppData\Roaming\.minecraft\runtime\jre-legacy\windows\jre-legacy\bin\javaw.exe - log4j-api-2.8.1.jar

Additionally looking into IIS logs, we observed some inbound reconnaissance attempts on the host "EC2AMAZ". We have not observed any outbound connections and investigating surrounding activities did not reveal any signs of active exploitation.

We have also performed a proactive threat hunt for exploitation of the Log4Shell vulnerability CVE-2021-44228 occurring on VMware Horizon Server and the MTR team did not identify malicious activity.

We will continue to monitor your environment and alert you to any malicious activity detected.

At this time, we recommend performing the below-referenced remediation steps as soon as possible. If you have any questions regarding this escalation, please reply to this email.

// Recommendations:

- If you are using Java 8 (or later) then you should upgrade Log4j to release 2.17.1 and Java 7 users should upgrade to release 2.12.4. Otherwise, in any release other than 2.16.0, you may remove the JndiLookup class from the classpath: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`
 - Refer: <https://logging.apache.org/log4j/2.x/security.html>
- In circumstances where it's not possible to update from an affected version, the following mitigations can be considered:
 - Restrict or isolate these systems from the Internet until patching is possible.
 - Implement outbound network filtering to restrict LDAP, LDAPS, and RMI traffic originating from servers to the Internet.
 - Ensure WAF and IPS rules are on the latest content versions to help with prevention monitoring and response.
- If the patching activity is not planned in the near future then please consider blocking the IPs mentioned, if there are no business dependencies associated, as they have been observed to be scanning for the Log4j vulnerability in your environment.
 - 45[.]155[.]205[.]233
 - 195[.]251[.]41[.]139
 - 45[.]130[.]229[.]168
 - 191[.]232[.]38[.]25
 - 5[.]157[.]38[.]50
 - 138[.]197[.]72[.]76
 - 45[.]83[.]64[.]1
 - 195[.]54[.]160[.]149
 - 45[.]146[.]164[.]160
 - 162[.]55[.]90[.]26
 - 31[.]131[.]16[.]127
 - 167[.]71[.]175[.]10
- Please notify the MTR team about your Findings and Actions.

// References:

- <https://logging.apache.org/log4j/2.x/security.html>
- <https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592>
- <https://github.com/NCSC-NL/log4shell/blob/main/software/README.md>
- <https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce>
- <https://news.sophos.com/en-us/2021/12/17/log4shell-response-and-mitigation-recommendations>

24.02.2022

Broadcasted email



[Security Advisory] - Cyber Resiliency During the Ukraine and Russia Conflict

// Overview

The Sophos MTR team has been monitoring the situation between Ukraine and Russia and with the conflict escalating, have been staying alert and vigilant in monitoring and protecting our customers. We have thus far not seen an increase in malicious cyber activity targeting our customers but will continue to stay informed and disseminate information as it becomes relevant.

The information below from the Cybersecurity & Information Agency [CISA], provides guidance and resilience recommendations for organizations in the wake of cyber attacks affecting Ukraine. CISA suggests organizations adopt a heightened cybersecurity posture while protecting their most critical assets.

// What you should do

Review the information from the Cybersecurity & Information Agency [CISA] - Shields Up advisory (<https://www.cisa.gov/shields-up>), which includes guidance for organizations of all sizes.

Recommendations include:

- Validate that all remote access to the organization's network requires multi-factor authentication
- Ensure that software and applications are up to date
- Confirm that unnecessary ports and protocols have been disabled on the network
- Test and ensure that backup procedures allow for critical data to be rapidly restored

Also ensure that all devices within your estate are properly protected and configured with Sophos MTR and that your contacts and response preferences have been set appropriately in Sophos Central.

// What Sophos MTR is doing

The MTR Operations team is actively monitoring our customers' environments 24/7 for active attacks against their estates. Should our team identify suspicious activity, they will respond according to the set response preferences.

While our team is constantly performing threat hunting across the various data we collect, we have initiated focused hunting campaigns around this conflict using gathered intelligence.

Lastly, our intelligence teams are actively monitoring the event and should any new cyber activity emerge, the intelligence will be immediately fused into our ongoing processes.

// Resources

CISA | Shields Up

- <https://www.cisa.gov/shields-up>

Sophos MTR Operations Team

MDR Interaktion



■ Reports

- Wöchentlich
- Monatlich

■ Bei dringenden Fällen direkte Kontaktaufnahme

■ Cases werden automatisch im MDR Dashboard erzeugt

■ MDR Team unternimmt regelmäßige Threat Hunts

■ Empfehlungen zur Verbesserung der Sicherheit

The screenshot displays a Sophos MDR case overview and the associated email content. The case is titled "Threat Hunt - Log4j VMWare Horizon" and is marked as "Resolved".

Overview:

Field	Value
Case ID	106066
Description	Threat Hunt - Log4j VMWare Horizon
Severity	3
Created on	Feb 5, 2022 at 9:30 AM
Resolved on	Feb 10, 2022 at 4:27 AM
Updated on	Feb 18, 2022 at 12:00 AM
Assigned on	Feb 5, 2022 at 9:30 AM
Type	Hunt
Status	Resolved
MITRE tactics	INITIAL_ACCESS
Escalated	Yes
Case synopsis	The MTR team conducted an investigation across the estate for indications of vulnerable Log4j instances. After investigation, the MTR team did not identify malicious activity associated with the critical vulnerability in Apache Log4j. However, we identified instances of log4j which require patching. Escalated to customer with recommendations

Devices [4]:

- Win10-4
- Win10-1
- Win10-2
- EC2AMAZ

Detections [0]

Email Content:

Team,
Case ID: 2-106066
Date: 2022-02-05 09:30:16 UTC
// Analysis:
We have conducted an investigation across your environment for indications of vulnerable Log4j instances. After investigation, the MTR team did not identify malicious activity associated with the critical vulnerability in Apache Log4j. However, we identified the following instances of log4j which require your attention as some of them are End of Life and some are vulnerable to CVE-2021-44228.
Format Below: Hostname - Path - Log4j Version
• Win10-1 - C:\xilinx\xic\tps\win64\jre\bin\java.exe - log4j-1.2.15.jar
• Win10-2 - C:\Users\armando.taveras\Downloads\arduino-1.8.16-windows\arduino-1.8.16\java\bin\javaw.exe - log4j-api-2.12.0.jar
• Win10-4 - D:\USERDATA\miguel.garabito\AppData\Roaming\.minecraft\runtime\jre-legacy\windows\jre-legacy\bin\javaw.exe - log4j-api-2.8.1.jar
Additionally looking into IIS logs, we observed some inbound reconnaissance attempts on the host "EC2AMAZ". We have not observed any outbound connections and investigating surrounding activities did not reveal any signs of active exploitation.
We have also performed a proactive threat hunt for exploitation of the Log4Shell vulnerability CVE-2021-44228 occurring on VMware Horizon Server and the MTR team did not identify malicious activity.
We will continue to monitor your environment and alert you to any malicious activity detected.
At this time, we recommend performing the below-referenced remediation steps as soon as possible. If you have any questions regarding this escalation, please reply to this email.
// Recommendations:
• If you are using Java 8 (or later) then you should upgrade Log4j to release 2.17.1 and Java 7 users should upgrade to release 2.12.4. Otherwise, in any release other than 2.16.0, you may remove the JndiLookup class from the classpath: zip -q -d log4j-core-*.jar
o Refer: <https://logging.apache.org/log4j/2.x/security.html>
• In circumstances where it's not possible to update from an affected version, the following mitigations can be considered:
o Restrict or isolate these systems from the Internet until patching is possible.
o Implement outbound network filtering to restrict LDAP, LDAPS, and RMI traffic originating from servers to the Internet.
o Ensure WAF and IPS rules are on the latest content versions to help with prevention monitoring and response.
• If the patching activity is not planned in the near future then please consider blocking the IPs mentioned, if there are no business dependencies associated, as they have been observed to be scanning for the Log4j vulnerability in your environment.
o 45[1155[1205[1233
o 195[1251[141[1139
o 45[1130[1229[1168
o 191[1232[138[125
o 5[1157[138[150
o 138[1197[172[176
o 45[183[164[11
o 195[154[1160[1149
o 45[1146[1164[1160
o 162[155[190[126
o 37[1131[116[1127

Sophos Detection and Response

Neuerungen in 2022/23

Kunden/Partner



Extended Detection and Response Endpoint, Servers, Firewall, Cloud Workloads, Email, Mobile und mehr – alles aus Sophos Central verwaltet

Sophos Service



24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service

Dritthersteller Integrationen

Firewall



FORTINET



Endpoint



Microsoft



McAfee



Symantec



Azure



aws



Google Cloud



Microsoft

Ping
Identity

okta

Cloud



Microsoft



TREND
MICRO

proofpoint

Email

IAM

Die nächsten Schritte



Solution Brief: IT-SiG 2.0

In diesem Solution Brief erfahren Sie, welche Anforderungen kritische Infrastrukturen bei der IT-Sicherheit erfüllen müssen, wie Sie die für KRITIS-Betreiber geforderten Sicherheitsvorkehrungen umsetzen uvm.

[Jetzt downloaden](#)



Podcast

Cybersecurity für kritische Infrastrukturen – was KRITIS-Unternehmen aus gesetzlicher Sicht beachten müssen mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB.

[Zum Podcast](#)



IT-Sicherheitsgesetz und Kritis

Das neue IT-Sicherheitsgesetz 2.0 betrifft nicht nur KRITIS-Betreiber in Deutschland, sondern auch deren Lieferanten in anderen Ländern. Weitere Informationen erhalten Sie auf unserer Webseite.

sophos.de/it-sicherheitsgesetz



Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

sophos.de/kontakt

